IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE SEARCHES OF DEVICES ASSOCIATED WITH: **MARC ELIASSAINT**	**Case No.** 1:24-mj-00062 1:24-mj-00063 1:24-mj-00064 1:24-mj-00065

AFFIDAVIT IN SUPPORT OF APPLICATIONS FOR SEARCH WARRANTS FOR (1) APPLE IPHONE, IMEI 357270098511411; (2) APPLIE IPHONE, IMEI 352842113627912; (3) A SANDISK USB DRIVE (NO SERIAL NUMBER); AND (4) A SEAGATE PORTABLE HARD DRIVE, SERIAL NUMBER NA5ADM6K

I, Sean Williams, a Special Agent with the U.S. Department of the Treasury, Treasury Inspector General for Tax Administration ("TIGTA"), being duly sworn, state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of four electronic devices that are currently in law enforcement's possession in the State of Maryland, as described in Attachments A-1 through A-4, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the U.S. Department of the Treasury, Treasury Inspector General for Tax Administration ("TIGTA"). TIGTA is tasked with ensuring the integrity of the IRS and its infrastructure security and protecting the IRS against external attempts to corrupt tax administration. TIGTA Special Agents are certified criminal investigators with authority to carry firearms, make arrests, execute warrants, and administer oaths. I am assigned as a Criminal Investigator within the Cybercrime

Investigations Division, whose mission is focused on communications- and computer network-related investigations. I have been employed by TIGTA since 2018. Prior to my employment with TIGTA, I was a Special Agent, Investigator, and Police Officer with multiple U.S. Federal Government agencies. I have received training from the National Cyber-Forensics and Training Alliance, Magnet Forensics, Cellebrite, and TIGTA's Cybercrimes Investigations Division. Through my training and experience with these types of investigations, I have encountered a number of situations the Internet and technical matters have been employed to conduct criminal activity.

3. This Affidavit is based on my own personal knowledge, training, and experience, as well as information provided to me by other law enforcement officers and witnesses, and my review of documents, reports, and records during the course of this investigation. I have not included in this Affidavit each and every fact known to me about this investigation. Rather, I have included only enough facts sufficient to establish probable cause for the issuance of the requested warrant.

ITEMS TO BE EXAMINED

4. The property to be searched includes four electronic devices seized (the "**Devices**") during the execution of a search warrant on 6436 Pomeroy Circle, Orlando, FL 32810 (the "Premises") on July 21, 2021, which are more specifically described in Attachments A-1 through A-4. These Devices, which are currently located in the District of Maryland, are the following:

a. Apple iPhone, IMEI 357270098511411

b. Apple iPhone, IMEI 352842113627912

c. Sandisk USB drive (no serial number)

d. Seagate portable hard drive, Serial Number NA5ADM6K

5. The TIGTA Cybercrime Investigations Division ("CCID") is headquartered in Lanham, MD. Due to the nature of cybercrimes, the subjects involved in the investigations can be located anywhere in the world. When conducting search warrants and seizing evidence from either physical locations or images from online accounts, the evidence, whether physical or electronic, is stored at the Lanham, MD location. The digital forensics analysts within TIGTA CCID are also located in Lanham, MD and it is necessary for the devices and account images to also be stored there for the analysts to perform extraction and analysis.

6. The applied-for warrant would authorize the search of stored data particularly described in Attachment B.

THE CARES ACT

7. The CARES Act is a federal law enacted on March 29, 2020, designed to provide emergency financial assistance to the millions of Americans who are suffering the economic effects caused by the COVID-19 pandemic. One source of relief provided by the CARES Act was the authorization of up to $349 billion in Small Business Administration ("SBA")-guaranteed forgivable loans to small businesses through the Paycheck Protection Program ("PPP"). In April 2020, Congress authorized over $300 billion in additional PPP funding.

8. The PPP allows qualifying small businesses and other organizations to receive loans with a maturity of two years and an interest rate of 1 percent. PPP loan proceeds must be used by businesses on payroll costs, interest on mortgages, rent, and utilities. The PPP allows the interest and principal to be forgiven if businesses spend the proceeds on

these expenses within eight weeks of receipt and use at least 75 percent of the forgiven amount for payroll.

9. The provisions of the CARES Act, in conjunction with an officially declared disaster by the United States Government, allowed for the SBA to offer Emergency Injury Disaster Loan ("EIDL") funding to business owners negatively affected by the COVID-19 pandemic. Using the SBA online portal, EIDL applicants submit personal and business information in support of each EIDL application, and do not have to submit supporting documentation of any sort.

10. The application includes a jurat-like paragraph where the applicant affirms that the information submitted is true and correct under the penalty of perjury and applicable criminal statutes. The application process involves filling out assorted data fields relating to the size of the affected business entity, the ownership of said business, and other information such as the number of employees and gross business revenues realized in the 12 months prior to COVID-19's impact on the national economy. This information, submitted by the applicant, is then used by SBA systems to calculate the principal amount of money the small business is eligible to receive in the form of an EIDL. However, in conjunction with the submission of an EIDL application, by simply clicking on and checking a box within the on-line application, an applicant may request and then receive up to $10,000 in an EIDL Cash Advance Grant based on the number of employees claimed. The EIDL Cash Advance Grant need not be repaid to the SBA if the loan application is ultimately denied by the SBA, or if the applicant declines the EIDL that may be offered by the SBA at a later date.

11. The SBA Office of Disaster Assistance ("ODA") controls the EIDL program and is headquartered at 409 3rd Street SW, Washington, DC 20416. The ODA has authority over all loans created and disbursed under the EIDL program. EIDL principal proceeds and available Cash Advance Grants (up to $10,000) are solely funded by the SBA and are disbursed from government-controlled accounts maintained with the U.S. Treasury at Federal Reserve Banks throughout the United States.

12. Pursuant to the provisions governing the EIDL program, loan proceeds must be used by that business on certain permissible expenses. The EIDL (working capital) loans may be used by the afflicted business, which must have existed in an operational condition on February 1, 2020, to pay fixed debts, payroll, accounts payable, and other bills that could have been paid had the COVID-19 disaster not occurred.

13. As explained below, multiple PPP and EIDL applications were submitted by an individual at the Premises to Celtic Bank and the SBA, using fabricated and/or fictitious documentation in order to fraudulently obtain funds from the federal government.

PROBABLE CAUSE

14. Between approximately February 3, 2020 through April 11, 2020, IP address 76.26.224.28 ("IP 28") was used to create accounts in the IRS Portal using over 125 different Social Security Numbers ("SSNs"). During the same time period, IP 28 was also used to file over 130 Federal Tax returns with MARC ELIASSAINT on file as the paid preparer.

15. Between approximately June 30, 2020 and July 31, 2020, one or more individuals from inside the Premises applied for over 65 loans from the SBA. Data retrieved from the SBA showed that all of the loans were applied for from the same IP address, IP 28.

A subpoena return from Comcast Communications revealed that during that time period, IP 28 was registered to A.D., and the service address for IP 28 was the Premises. A check of the Premises on the Orange County Property Appraiser's website was conducted in 2021 and showed that the website listed MARC ELIASSAINT, C.D., and A.D. as co-owners of the Premises.

16. Between approximately July 30, 2020 and December 23, 2020, one or more individuals from inside the Premises applied for 19 loans from the SBA. Data retrieved from the SBA showed that all of the loans were applied for from the same IP address, 2601:882:4000:1a00::/60 ("IP 2601"). A subpoena return from Comcast Communications revealed that during this time period, IP 2601 was registered to A.D., and the service address for IP 2601 was the Premises. A check of the Premises on the Orange County Property Appraiser's website showed that the website listed MARC ELIASSAINT, C.D., and A.D. as co-owners of the Premises.

I. 360 Tax Services, LLC

17. On or about June 8, 2020, ELIASSAINT, from inside the Premises[1], applied for a PPP loan number 9350357801 in the amount of $432,500 on behalf of 360 Tax Services, LLC (EIN: 47-5322688). ELIASSAINT is listed as the sole owner of 360 Tax Services, LLC on the loan documents.

18. The loan application represented that the business had started in 2015 and identified the purpose of the PPP loan as "payroll, lease/mortgage interest, and utilities."

[1] SBA data showed that this loan was applied for from IP 28.

The loan application identified the average monthly payroll of the business as $173,000 for eight employees.

19. On June 9, 2020, the JPMorgan Chase account held in the name of 360 Tax Services, LLC received a deposit of $432,500.

20. On February 1, 2021, ELIASSAINT completed a second draw application[2] for first draw loan number 9350357801 for $66,715. The application was for a 360 Tax Services, LLC (EIN: 47-5322688). ELIASSAINT identified himself as the primary contact and sole owner of 360 Tax Services, LLC. The loan application represented that the business had started in 2015, and identified the purpose of the PPP loan as "payroll costs, rent/mortgage interest, utilities, covered operations expenditures, and covered supplier costs." The loan application identified the average monthly payroll of the business as $26,686 for nine employees. On February 4, 2021, the JPMorgan Chase account held in the name of 360 Tax Services, LLC received a deposit of $66,715.

21. ELIASSAINT electronically signed the PPP Borrower Application Forms for 360 Tax Services, LLC. In addition, the loan application contained ELIASSAINT's initials, M.E., to certify each of the following representations:

a. The Applicant business was in operation on February 15, 2020 and had employees for whom it paid salaries and payroll taxes or paid independent contractors, as reported on Form(s) 1099-MISC;

[2] PPP allows certain eligible borrowers that previously received a PPP loan to apply for a Second Draw PPP loan with the same general loan terms as their First Draw PPP loan.

b. The funds will be used to retain workers and maintain payroll or make mortgage interest payments, lease payments, and utility payments, as specified under the Paycheck Protection Program Rule; and

c. The information provided in the application and all supporting documents and forms is true and accurate in all material respects.

22. Agents have identified multiple falsified documents that ELIASSAINT submitted in connection with the loan application. Specifically, ELIASSAINT submitted a falsified IRS Form 941 (quarterly tax return) for the first quarter of 2019. This Form 941 lists the EIN for 360 Tax Services, LLC. Based on IRS records, 360 Tax Services, LLC completed IRS Form 941s for the third and fourth quarters of 2020, as well as an IRS Form 940 (annual tax return) for 2020, which claimed that $319,483.85 was paid to employees in 2020. No returns exist for the first or second quarters of 2020 or the years of 2019, 2018, or 2017.

23. Based on Florida Department of Revenue records, 360 Tax Services, LLC became inactive for Re-employment Assistance Tax ("RT") during the first quarter of 2016. 360 Tax Services, LLC was reinstated for RT on June 20, 2020 and claimed nine employees with wages totaling $319,483.85 from July 1, 2020 through December 31, 2020.

24. Records from the JPMorgan Chase account held in the name of 360 Tax Services, LLC, with ELIASSAINT as the only signature authority, revealed electronic withdrawals for "Payroll" in 2016 totaling $9,520.55. There were no withdrawals for "Payroll" in 2017, 2018, 2019, or the first six months of 2020. From July 10, 2020 through November 27, 2020, bi-weekly withdrawals totaling $248,600.30 were made for "Payroll." Additionally, withdrawals were made via ATMs, payments were made to Caliber Home

Loan and LA Fitness, and purchases were made at various businesses including Home Depot, Wal-Mart, Speedway, JC Penney, Sears, Orange Blossom Liquor, Tesla, and a multitude of restaurants.

II. 360 Florida Home, LLC

25. On July 9, 2020, ELIASSAINT completed application number 3309762599 for an EIDL for $54,000. An advance of $10,000 was also requested, approved, and sent to a Wells Fargo bank account, xxxxxxx973. The application was for a business registered in ELIASSAINT's name, 360 Florida Home, LLC, with the address listed as the Premises. ELIASSAINT identified himself as the primary contact and sole owner of 360 Florida Home, LLC. The loan application represented that the business had started in 2018. The loan application claimed $13,333 in monthly revenue and ten employees. The loan was declined because ELIASSAINT did not provide the requested documents to the SBA (e.g. identification, Form 1099, Schedule C, bank statements, Form 941).

26. Based on IRS records, 360 Florida Home, LLC has not completed an IRS Form 941 (quarterly tax returns) for any tax year.

27. Based on Florida Secretary of State records, 360 Florida Home, LLC became inactive in September 2019, due to a failure to file an annual report. Based on Florida Department of Revenue records, 360 Florida Home, LLC had no record on file for filing for Re-employment Assistance Tax ("RT").

III. The Premises Identified as ELIASSAINT's Home

28. In or about July 2021, agents identified the Premises as ELIASSAINT's home and business address based on Florida DMV records, Orange County (FL) Property Appraiser ("OCPA") records, banking records, and IP information. First, Florida DMV

records revealed that ELIASSAINT's Florida driver's license was issued on May 8, 2017, and listed the Premises as his address. Additionally, multiple vehicles registered in ELIASSAINT's name also listed the Premises as the address of record, including a vehicle registered on January 26, 2021.

29. Second, records from the OCPA revealed ELIASSAINT as the listed owner of the Premises since August 5, 2016.

30. Third, records from Wells Fargo bank accounts listed the Premises as ELIASSAINT's home address, and IP 28 was used to access one of the accounts as recently as February 2021.

31. Fourth, records from JPMorgan Chase bank accounts listed the Premises as the address for 360 Tax Services, LLC, and IP 28 was used to access the account as recently as March 15, 2021.

32. Finally, based on IRS records, IP 28 was used to access ELIASSAINT's information in the IRS Portal, file Federal Tax Returns in the name of ELIASSAINT (with the Premises as the address of record), and apply for an SBA EIDL in the name of one of ELIASSAINT's businesses. IP 28 is controlled by Comcast Communications. Based on information from Comcast Communications, this IP address was subscribed to the Premises in 2020, and as recently as February 2021, including during the period when the above accesses occurred.

IV. The Search Warrant at 6436 Pomeroy Circle

33. On July 21, 2021, TIGTA executed a search warrant at ELIASSAINT's residence, located at 6436 Pomeroy Circle, Orlando, FL 32810.

34. During the search of the residence, agents discovered equipment that is

consistent with the manufacturing of fraudulent identifications. This equipment included blank identification cards, holograms, a card embosser, and a card printer cleaning kit.

35. That search warrant permitted TIGTA to seize the **Devices** and to seize from them evidence of violations of 18 U.S.C. §§ 1343 (wire fraud), 1349 (conspiracy to commit wire fraud, 1001 (false statements), and 1956 (money laundering). That warrant did not specifically provide for the seizure from the **Devices** of evidence of 18 U.S.C. §§ 1028 (identity theft), 1028A (aggravated identity theft), 1029 (fraud and related activity in connection with access devices), and 1030 (fraud and related activity in connection with computers) (the "**Subject Offenses**"). Following the execution of the search warrant, TIGTA initially examined the **Devices** for evidence of the violations specified in the search warrant on or about July 25, 2023 and September 15, 2023. TIGTA now seeks to examine the **Devices** for evidence of the Subject Offenses. Thus, in the abundance of caution, the United States is seeking this additional search warrant.

36. The **Devices** are currently in the lawful possession of TIGTA in Lanham, MD and the evidence seized during the search warrant was sent to the Lanham, MD location for evidence storage, image extraction, and analysis.

37. In my training and experience, I know that the **Devices** are stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the **Devices** first came into TIGTA's possession.

V. Evidence of Identity Theft and Computer Fraud Observed

38. During the initial examination of the **Devices** for evidence of violations of 18 U.S.C. §§ 1001, 1014, 1343, 1349, and 1956, as outlined in the search warrants in Case

Nos. 6:21-mj-1570 (M.D. Fla.) and 6:21-mj-1571 (M.D. Fla.), evidence consistent with identity theft was observed. The **Devices** contained conversations between the owner of the **Devices** and co-conspirators discussing purchasing materials to make fraudulent identifications, purchasing "ID and SSN," making identification cards, and the sharing of Personally Identifiable Information ("PII").

39. First, an Apple iPhone, IMEI 357270098511411, contained messages sent from the owner of the device that included the sharing of PII.

40. Second, an Apple iPhone, IMEI 352842113627912, contained messages sent from the owner of the device that included the sharing of PII. It also contained a message sent from the owner of the device on July 13, 2021 that read, "How many id u want me make" and, "Send me the name and date of birth for all 5".

41. Third, a SanDisk USB drive (no serial number) contained PII, copies of identifications, fraud tutorials, fraudulent carding information, TOR browser, evidence of hacking, and software and visits known to be associated with the dark web.

42. Fourth, a Seagate portable hard drive, Serial Number NA5ADM6K, contained PII, pirated software used to make fraudulent identification, TOR browser, and evidence of hacking.

43. In my training and experience, the existence of this type of information is consistent with evidence of identity theft and fraud and related activity in connection with computers.

TIME OF EXECUTION

44. Because this warrant seeks permission only to examine information on computer media in law enforcement's possession, the execution of this warrant does not

involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize the search of the data within the warrant at any time in the day or night.

CONCLUSION

45. Based on the facts as outlined above, your affiant respectfully submits that there is probable cause to believe that evidence, fruits and/or instrumentalities of the **Subject Offenses** will be located on the **Devices** (more particularly described in Attachment A).

46. I declare under the penalty of perjury that the foregoing is true and correct to the best of my knowledge, information, and belief.

Respectfully Submitted,

Sean Williams
Special Agent Sean Williams
Treasury Inspector General for
Tax Administration

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 10th day of January, 2024.

United States District Court
For The District Of Maryland

Honorable Erin Aslan
United States Magistrate Judge

ATTACHMENT A-1

Property to Be Searched

The property to be searched is an Apple iPhone, IMEI 357270098511411.

This Device is currently in the lawful possession of TIGTA located at the TIGTA CCID office located at 5000 Ellin Road, Lanham, MD 20607. This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT A-2

Property to Be Searched

The property to be searched is an Apple iPhone, IMEI 352842113627912.

This Device is currently in the lawful possession of TIGTA located at the TIGTA CCID office located at 5000 Ellin Road, Lanham, MD 20607. This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT A-3

Property to Be Searched

The property to be searched is a Sandisk USB drive (no serial number), black and red in color.

This Device is currently in the lawful possession of TIGTA located at the TIGTA CCID office located at 5000 Ellin Road, Lanham, MD 20607. This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT A-4

Property to Be Searched

The property to be searched is a Seagate portable hard drive, Serial Number NA5ADM6K.

This Device is currently in the lawful possession of TIGTA located at the TIGTA CCID office located at 5000 Ellin Road, Lanham, MD 20607. This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

PARTICULAR THINGS TO BE SEIZED

All records contained in the items described in Attachment A which constitute evidence of violations of 18 U.S.C. §§ 1028 (identity theft), 1028A (aggravated identity theft), 1029 (fraud and related activity in connection with access devices), and 1030 (fraud and related activity in connection with computers) as outlined below:

1. All records relating to violations of 18 U.S.C. §§ Sections 1028 (identity theft), 1028A (aggravated identity theft), 1029 (fraud and related activity in connection with access devices), and 1030 (fraud and related activity in connection with computers) (the "**Subject Offenses**"), those violations involving MARC ELIASSAINT occurring on or after, January 1, 2016, specifically:

a. Records and information relating to identity theft, trafficking in stolen identities, and fraud involving the unauthorized use of personally identifiable information ("PII"), including but not limited to credit and debit cards and associated statements, other bank statements and records, receipts, checks, and identity documents such as driver's licenses and social security cards;

b. Records and information relating to bank accounts used in furtherance of, or relating to, violations of the **Subject Offenses**;

c. Records and information relating to the identity, state of mind, or location of the suspects;

d. Records and information relating to communications and any IP addresses used in furtherance of, or relating to, violations of the **Subject Offenses**; and

e. Communications between and among MARC ELIASSAINT and/or other co-conspirators regarding the theft, trafficking, and/or fraudulent use of PII.

With respect to the search of the information provided under this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable.

If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.